대한민국 특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2001년 제 64186 호
Application Number PATENT-2001-0064186

출 원 년 월 일 : 2001년 10월 18일
Date of Application OCT 18, 2001

CERTIFIED COPY OF PRIORITY DOCUMENT

출 원 인 : 한국전자통신연구원
Applicant(s) KOREA ELECTRONICS & TELECOMMUNICATIONS RESEARCH INS

2002 년 01 월 10 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0003

【제출일자】 2001.10.18

【발명의 명칭】 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법

【발명의 영문명칭】 METHOD FOR MODIFYING AUTHORITY OF A CERTIFICATE OF AUTHENTICATION USING INFORMATION OF A BIOMETRICS IN A PKI INFRASTRUCTURE

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【성명】 장성구

【대리인코드】 9-1998-000514-8

【포괄위임등록번호】 2001-038646-2

【대리인】

【성명】 김원준

【대리인코드】 9-1998-000104-8

【포괄위임등록번호】 2001-038648-7

【발명자】

【성명의 국문표기】 노종혁

【성명의 영문표기】 ROH,Jong-Hyuk

【주민등록번호】 700420-1143627

【우편번호】 405-840

【주소】 인천광역시 남동구 구월3동 1376-7

【국적】 KR

【발명자】

【성명의 국문표기】 김태성

【성명의 영문표기】 KIM,Taesung

【주민등록번호】 721202-1221829

【우편번호】 305-803

【주소】 대전광역시 유성구 송강동 200-1 한솔아파트 203-705
【국적】 KR
【발명자】
【성명의 국문표기】 김희선
【성명의 영문표기】 KIM,Hee Sun
【주민등록번호】 751015-2262118
【우편번호】 305-350
【주소】 대전광역시 유성구 가정동 236-1 구 332
【국적】 KR
【발명자】
【성명의 국문표기】 최대선
【성명의 영문표기】 CHOI,Dae Seon
【주민등록번호】 730302-1069411
【우편번호】 302-280
【주소】 대전광역시 서구 월평동 황실타운 118-905
【국적】 KR
【발명자】
【성명의 국문표기】 조영섭
【성명의 영문표기】 CHO,Young Seob
【주민등록번호】 691212-1155513
【우편번호】 305-804
【주소】 대전광역시 유성구 신성동 142-11 상가주택 301호
【국적】 KR
【발명자】
【성명의 국문표기】 조상래
【성명의 영문표기】 CHO,Sang Rae
【주민등록번호】 711023-1037015
【우편번호】 305-752
【주소】 대전광역시 유성구 송강동 송강청솔아파트 512-1408
【국적】 KR

【발명자】

【성명의 국문표기】 진승헌

【성명의 영문표기】 JIN,Seung Hun

【주민등록번호】 680723-1037010

【우편번호】 302-752

【주소】 대전광역시 서구 월평2동 백합아파트 104동 1405호

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인
장성구 (인) 대리인
김원준 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	3 면	3,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	11 항	461,000 원
【합계】	493,000 원	
【감면사유】	정부출연연구기관	
【감면후 수수료】	246,500 원	

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서의 권한 변경 방법에 관한 것이다. 즉, 본 발명은 공개키 기반 구조 인증시스템에서 인증서의 폐지, 중지, 회복 등과 같은 인증서의 권한 변경을 위한 사용자 인증 필요시 생체정보를 이용하여 신뢰성이 보장된 사용자 인증을 수행할 수 있게 됨으로써, 종래와 같이 인증서 권한 변경을 위해 사용자가 등록기관이나 인증기관을 직접 찾아가지 않아도 되며, 인증기관과 온라인 연결된 각자의 사용자 시스템을 이용하여 쉽게 인증서 권한 변경 작업을 수행할 수 있게 되는 이점이 있다.

【대표도】

도 5

【색인어】

공개키, 인증시스템, 생체정보, 인증서 폐지, 인증서 정지, 인증서 회복

【명세서】

【발명의 명칭】

공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법
{METHOD FOR MODIFYING AUTHORITY OF A CERTIFICATE OF AUTHENTICATION USING INFORMATION OF A BIOMETRICS IN A PKI INFRASTRUCTURE}

【도면의 간단한 설명】

도 1은 본 발명의 실시 예에 따른 공개키 기반 구조 인증시스템의 네트웍 구성을 도시한 것이다.

도 2는 본 발명의 실시 예에 따른 사용자 시스템의 개략적인 블록 구성을 도시한 것이다.

도 3은 본 발명의 실시 예에 따른 인증기관 서버의 개략적인 블록 구성을 도시한 것이다.

도 4는 본 발명의 실시 예에 따른 사용자 시스템에서 인증서 권한 변경 요청시 동작 제어 흐름을 도시한 것이다.

도 5는 본 발명의 실시 예에 따른 인증기관 서버에서 인증서 권한을 변경시키는 동작 제어 흐름을 도시한 것이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 공개키 기반 구조(PKI: Public Key Infrastructure)에 관한 것으로, 특히 공개키 기반 구조 인증시스템에서 개인키의 손상에 따른 인증서의 정지, 회복, 폐기를 생체정보를 이용한 사용자의 인증을 통해 사용자 시스템과 인증기관간 온라인으로 수행할 수 있도록 하는 인증서 권한 변경 방법에 관한 것이다.

<7> 통상적으로, 공개키 기반 구조는, 인터넷상 보안이 요구되는 전자문서의 송/수신시 상기 인증시스템에 의해 인증된 회원 사용자간에 공개키와 개인키를 이용한 암호화 전송이 가능하도록 하는 시스템을 말하는 것으로, 즉, 상기 인증시스템에 회원 등록된 사용자들은 해당 인증기관으로부터 정당한 사용자임을 인증하는 디지털 인증서를 발급받고 상대방 공개키로 보안이 요구되는 전자문서를 암호화한 후, 자신의 개인키로 전자서명하여 전송함으로써 상기 인증시스템에 회원 등록된 사용자간에는 전자문서를 안전하게 송/수신할 수 있도록 하는 시스템을 말한다.

<8> 현재 공개키 기반 구조에서는 인증서와 관련된 작업/관리에 관련된 표준화된 프로토콜로 인증서 등록, 발급, 키소유증명, 갱신, 회복, 폐지 등을 위해 IETF에서 제안하고 있는 RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols(CMP)를 사용하고 있는데, 상기 CMP에서 사용

되는 메시지 포맷은 RFC 2511 CRMF(Certificate Request Message Format)을 사용하고 있으며, 인증서의 정지 또는 폐기 요청시 위조된 메시지인지를 확인하기 위하여 사용자로부터의 인증서 권한 변경 요청 메시지에 사용자의 개인키를 이용한 전자서명이 반드시 필요하도록 규정하고 있다.

<9> 그러나 종래 공개키 기반 구조 인증시스템에서는 사용자가 개인키를 소유한 경우에도 인증서의 회복을 위해서는 반드시 해당 등록기관이나 인증기관을 직접 방문하여야만 처리가 가능하며, 또한 사용자의 개인키가 손상되어 전자서명이 불가능하게 되는 경우 종래 공개키 기반 구조 인증시스템에서는 상기 인증서의 정지 및 폐지에 대해서도 온라인으로 처리가 불가능함에 따라 사용자의 신원을 증명하기 위해 사용자가 직접 해당 등록기관 또는 인증기관을 찾아가서 신원 인증을 통해 인증서 권한의 변경을 직접 요청하여야 하는 등 불편한 문제점이 있었다.

<10> 한편, 상기와 같은 공개키 기반 구조 인증시스템에서의 인증서 권한 변경 방법으로는 출원번호 1999-0051586호에 개시된 '인증기관 시스템의 사용자용 공개키 인증서 생성방법'과 2000년 10월에 출판된 'Telecommunications Review'지 제10권 5호 915~938페이지에 개시된 '공개키 기반구조의 연구개발 동향과 국내 표준규격' 등과 같은 공개키 기반 구조에 대한 기술이 개시되어 있으나, 상기 '인증기관 시스템의 사용자용 공개키 인증서 생성방법'에는 단지 인증기관에서 사용자에게 신속하게 공개키 인증서를 생성하는 방법이 개시되어 있으며, '공개키 기반구조의 연구개발 동향과 국내표준규격'에는 단지 공개키 구현에 필요한 표준 및 동향 파악과 국내 공개키 기반 구조를 위한 표준안이 개시되고 있을 뿐, 상기

한 공개키 기반 구조 인증시스템에서 개인키 손상시 인증서의 권한 변경을 위해서는 사용자가 직접 해당 등록기관이나 인증기관을 방문하여서 신원인증을 통해 변경 요청을 해야하는 불편함이 여전히 문제점으로 남아 있었다.

【발명이 이루고자 하는 기술적 과제】

<11> 따라서, 본 발명의 목적은, 공개키 기반 구조 인증시스템에서 개인키의 손상에 따른 인증서의 권한 정지, 권한 회복, 폐기를 생체정보를 이용한 사용자의 인증을 통해 사용자 시스템과 인증기관간 온라인으로 수행할 수 있도록 하는 인증서 권한 변경 방법을 제공함에 있다.

<12> 상술한 목적을 달성하기 위한 본 발명은 사용자의 신원을 대행 확인하는 등록기관, 상기 등록기관에 의해 신원 확인된 사용자에 대한 인증서를 발행하는 인증기관 및 사용자 시스템을 포함하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법에 있어서, (a)상기 인증시스템에 회원 등록된 사용자로부터 인증서 권한 변경 요청이 있는 경우 상기 인증기관 서버에 로그인하여 접속하는 단계; (b)상기 사용자 시스템에 구비된 생체정보 입력장치를 통해 사용자 인증을 위한 생체정보를 입력받는 단계; (c)상기 사용자의 요청에 따른 인증서 권한 변경 요청 메시지를 생성하는 단계; 및 (d)상기 생체정보와 인증서 권한 변경 요청 메시지를 상기 인증기관으로 전송하여 온라인으로 인증서 권한 변경을 요청하는 단계;를 포함하여 진행하는 인증서 권한 변경 요청 방법을 구현하며, (a')인터넷을 통해 상기 인증시스템에 접속한 사용자 시스템으로부터의 인증서 권한 변경 요청 메시지를 수신하는 단계; (b')상기 인증서 권한 변경을 요청한 사용자로부터 시스템 회원 인증을 위한 로그인 정보 및 생체정보를 입력받

는 단계; (c')상기 개인키를 통해 인증된 사용자의 데이터 베이스 저장부내 등록 생체정보와 상기 입력된 생체정보가 일치하는지 여부를 검사하는 단계; (d')상기 생체정보가 일치하는 경우 해당 사용자에게 발급된 인증서의 권한을 상기 인증서 권한 변경 요청에 맞게 변경시키는 단계; 및 (e')상기 인증서 권한 변경이 정상적으로 처리되었음을 알리는 응답메시지를 상기 사용자 시스템으로 전송하여 사용자에게 알리는 단계;를 포함하여 진행하는 인증서 권한 변경 방법을 구현하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<13> 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시 예의 동작을 상세하게 설명한다.

<14> 도 1은 본 발명의 실시 예에 따른 공개키 기반 구조 인증시스템의 네트웍 구성을 도시한 것이다. 이하 상기 도 1을 참조하면, 공개키 기반 구조 인증시스템은, 상기 인증시스템에 등록된 사용자에 대한 인증서를 발행하는 인증기관(108)과 사용자 시스템(104)으로 구성된다.

<15> 먼저 상기 사용자 시스템(104)은 PC(Personal Computer)등과 같이 인터넷(106)에 접속할 수 있는 단말장치를 말하는 것으로, 사용자는 상기 인증기관(108)에 회원 사용자로 등록하고, 상기 인증기관(108)으로부터 인증서를 발급 받은 후, 상기 사용자 시스템(104)을 이용하여 인터넷 뱅킹 또는 보안 웹메일 등 개인정보의 보안이 요구되는 인터넷 활동을 수행하며, 또한 부득이한 사정으로 인해 인증서의 권한을 변경하고자 하는 경우 상기 사용자 시스템(104)을 이용하

여 인증기관(108)에 접속한 후, 생체정보를 이용한 사용자 인증을 통해 온라인으로 인증서 권한 변경을 수행할 수 있게 된다.

<16> 특히, 본 발명의 실시 예에서는 종래 인증기관으로부터 발급받은 인증서의 권한을 변경하고자 하는 경우 해당 등록기관이나 인증기관으로 사용자가 직접 찾아가야 했던 문제점을 해결하고자, 인증기관(108)에 회원 등록시 지문정보 등과 같은 사용자(100)의 고유 생체정보를 사용자 정보와 함께 등록하고 상기 생체정보를 이용하여 보다 신뢰성 높은 사용자 인증 수행이 가능하도록 함으로써, 상기 인증시스템의 회원 사용자(100)가 상기 인증기관(108)과 온라인으로 연결된 각자의 사용자 시스템(104)을 이용하여 인증서의 권한 변경을 수행할 수 있도록 한다.

<17> 도 2는 상기 도 1에 도시된 사용자 시스템의 개략적인 블록 구성을 도시한 것이다. 상기 도 2를 참조하면, 제어부(204)는 상기 사용자 시스템의 전반적인 동작을 제어하며, 본 발명의 실시 예에 따라 상기 인증시스템 접속시 인증기관(108)으로부터 제공되는 인증시스템 회원 사용자를 위한 웹페이지 화면을 다운로드받아 모니터부(200)에 디스플레이시키며, 상기 인증기관(108)으로부터 인증서를 발급받은 회원 사용자로부터 인증서 폐지, 중지, 회복 등과 같은 인증서 권한 변경 요구가 있는 경우 사용자의 생체정보를 입력받아 상기 요청 메시지와 함께 인증기관(108)으로 전송시킨다.

<18> 메모리부(206)는 제어부(204)의 동작에 필요한 각종 운영 프로그램을 내장하며, 상기 운영 프로그램의 구동시 필요한 각종 기본 데이터를 저장하고 있는 롬(ROM:Read Only Memory)과 제어부(204)의 제어에 의해 동작되는 프로그램을 임

시 저장하거나 상기 동작 프로그램 수행시 발생되는 데이터를 일시 저장하기 위한 램(RAM:Random Access Memory)으로 구성된다. 통신부(208)는 상기 제어부(204)의 제어에 따라 상기 인증서 권한 변경 요청 메시지를 해당 인증기관(108)으로 전송시키며, 상기 인증기관(108)과 사용자 시스템(104)간 인터넷(106)을 통해 송/수신되는 데이터를 인터페이스한다. 키입력부(202)는 사용자 인터페이스부로 다양한 숫자키 및 기능키를 구비하며 사용자로부터의 키입력 발생시 해당 키 이벤트 데이터를 발생시켜 제어부(204)로 인가시킨다. 모니터부(200)는 제어부(204)의 제어에 따른 사용자 시스템의 각종 동작 상태를 디스플레이시킨다.

<19> 또한 본 발명의 실시 예에 따른 사용자 시스템(104)에는 사용자(100)의 생체정보를 입력할 수 있는 생체정보 입력장치로 지문정보 입력장치(102)가 구비되는데, 상기 지문정보 입력장치(102)는, 지문센서를 통해 사용자의 지문을 스캔 입력하는 지문인식부(214)와 상기 지문인식부(214)로부터 스캔 입력된 사용자 고유의 지문데이터를 분석하여 사용자 고유의 지문특징값을 추출하여 사용자 시스템(104)의 제어부(204)로 인가시키는 지문처리부(212)로 구성된다. 한편, 본 발명의 실시 예에서는 상기 생체정보 입력장치로 사용자의 지문을 인식하는 지문정보 입력장치를 예시하였으나, 이는 설명의 편의상 일 예를 들어 설명한 것 일뿐 상기 생체정보는 사용자의 홍체 정보나 얼굴특징 벡터값 등 다양한 사용자 고유의 생체정보가 될 수 있다.

<20> 인증기관(108)은 상기 공개키 기반 인증시스템의 핵심 객체로서 인증서 등록 발급 조회시 인증서의 정당성에 대한 관리를 총괄하는 시스템으로, 인터넷 뱅킹 등과 같이 보안이 요구되는 인터넷을 통한 전자문서의 송/수신시 상기 인증시

스템에 회원 등록된 사용자를 인증하는 디지털 인증서를 발행하여 공신력 있는 제3자의 인증서를 통한 보다 안정성 있는 전자문서 전송 서비스를 제공하며, 본 발명의 실시 예에 따라 사용자 시스템으로부터의 인증서 권한 변경 요청이 있는 경우 생체정보를 이용한 사용자 인증을 통해 해당 변경 요청에 따른 인증서 권한 변경을 수행한다.

<21> 도 3은 상기 도 1의 인증기관 서버(108)의 개략적인 블록 구성을 도시한 것이다. 이하 상기 도 3을 참조하여 인증기관 서버(108)의 동작을 보다 상세히 설명하기로 한다. 먼저 분석 모듈부(300)는 서버 제어부(302)의 제어에 따라 상기 사용자 시스템(104)으로부터 암호화되어 전송된 인증서 권한 변경 요청 메시지를 복호화시키고 상기 메시지의 무결성을 검사한다.

<22> 메시지 생성 모듈부(304)는 서버 제어부(302)의 제어에 따라 상기 인증서 권한 변경 요청 메시지에 대하여 해당 인증서 권한 변경이 정상적으로 수행되었음을 알리는 응답메시지 또는 생체정보의 불일치로 인한 인증서 권한 변경 수행에 에러가 발생했음을 알리는 오류메시지를 생성한다. 암호 모듈부(306)는 상기 메시지 생성모듈부(304)로부터 생성된 응답메시지 또는 오류메시지를 해당 사용자 시스템(104)의 공개키로 암호화시킨다. 서명 모듈부(308)는 상기 사용자 시스템(104)의 공유된 비밀키로 보호처리된 상기 응답메시지 또는 오류메시지를 인증기관(108)의 개인키로 전자서명을 수행한다.

<23> 서버 제어부(302)는 상기 인증기관 서버(108)의 전반적인 동작을 제어하며, 특히 본 발명의 실시 예에 따라 상기 인증시스템의 회원 사용자의 인증서 권한 변경 요청 수신시 해당 사용자 시스템(104)으로부터 전송된 회원 사용자의 생체

정보를 검사하여 회원 사용자에 대해 생체정보를 이용한 사용자 인증을 수행하며, 상기 인증서 권한 변경을 요청한 회원 사용자가 정당한 사용자로 판단되는 경우 상기 메시지 생성 모듈부(304)를 제어하여 인증서 권한 변경 요청이 정상적으로 처리되었음을 알리는 응답메시지를 생성시키고, 암호모듈부(306)와 서명모듈부(308)를 제어하여 상기 응답메시지를 공유된 비밀키로 보호처리하고, 인증기관 개인키로 전자서명을 수행하여 해당 사용자 시스템(104)으로 온라인 전송시킨다.

<24> 데이터 베이스 저장부(110)는 상기 인증기관 서버(108)에 의해 참조되며, 상기 인증시스템에 회원 가입된 사용자 정보를 구비한 사용자 정보 DB(310)와 상기 해당 사용자에 대한 생체정보를 상기 사용자 정보와 연계되도록 저장하고 있는 생체정보 DB(312) 등 상기 인증기관 서버(108) 운영에 따른 각종 DB를 구비한다. 메모리(314)는 서버 제어부(302)의 동작에 필요한 각종 운영 프로그램을 내장하며, 상기 운영 프로그램의 구동시 필요한 각종 기본 데이터를 저장하고 있는 롬(ROM:Read Only Memory)과 서버 제어부(302)의 제어에 의해 동작되는 프로그램을 임시 저장하거나 상기 동작 프로그램 수행시 발생되는 데이터를 일시 저장하기 위한 램(RAM:Random Access Memory)로 구성된다. 통신부(316)는 상기 서버 제어부(302)의 제어에 따라 상기 사용자 시스템(104)으로부터의 인증서 권한 변경 요청에 따른 응답메시지를 해당 사용자 시스템(104)으로 전송시키며, 상기 사용자 시스템(104)과 인증기관 서버(108)간 인터넷(106)을 통해 송/수신되는 데이터를 인터페이스한다.

<25> 도 4는 본 발명의 실시 예에 따라 상기 인증기관으로부터 인증서를 발급 받은 회원 사용자가 사용자 시스템(104)을 이용하여 상기 인증기관(108)으로 인증서 권한 변경 요청을 수행하기 위한 동작 제어 흐름을 도시한 것이다. 이하 상기 도 1, 도 2 및 도 4를 참조하여 상세히 설명한다.

<26> 먼저 지정된 등록기관을 통해 상기 인증기관(108)에 회원으로 등록한 사용자는 이후 자신의 사용자 시스템(104)을 이용하여 상기 인증기관(108)에 접속한 후, 상기 회원 등록에 따라 인증기관으로부터 부여된 참조번호와 생체정보를 이용한 사용자 인증을 통해 자신의 공개키에 대한 인증서를 발급 받게 된다. 상기 인증서는 공신력있는 제3자인 인증기관이 상기 회원 가입한 사용자에 대한 신원을 보증하여 주는 문서로 해당 사용자의 공개키 정보를 인증기관 개인키로 전자서명하여 발급하여 주게 되는데, 회원 사용자들은 상기 인증서를 이용하여 상대방의 공개키를 확인할 수 있는 등 보안 서비스를 수행하는 동안 중요한 요소로써 사용되게 된다.

<27> 이러한 인증서는 전술한 바와 같이 사용자의 요청에 따라 정지, 폐지 또는 회복 등으로 처리 가능하게 되는데, 사용자는 발급 받은 인증서에 대해 인증서의 정지, 폐지, 회복을 수행하고자 하는 경우 상기 인증시스템에 접속하여 상기 인증기관(108)으로 이와 같은 요청메시지를 전송하여 원하는 작업을 수행하게 된다.

<28> 즉, 사용자 시스템(104)은 사용자로부터 상기 인증시스템의 접속 요구가 있는 경우 (S400)단계에서 인터넷(106)으로 연결된 상기 인증시스템에 사용자의 로그인 정보를 이용하여 온라인 접속한 후, 인증기관(108)에서 회원 인증된 사용자

들에게 제공하는 보안 서비스를 위한 웹페이지 화면을 모니터부(200)를 통해 디스플레이시킨다. 이때 상기 웹페이지 화면은 회원 인증된 사용자들이 각종 보안 서비스 관련 메뉴와 인증서 관련 정보 변경 메뉴 등 다양한 기능 수행을 위한 메뉴로 구성될 수 있다.

<29> 따라서 사용자는 상기 웹페이지 화면에서 인증서 권한 변경을 위한 메뉴 중 원하는 메뉴를 선택하여 인증서 권한 변경을 요청하게 되는데, 즉 사용자가 더 이상 인증서를 필요로 하지 않게 되어 인증서를 폐지하고자 하는 경우에는 인증서 폐지 메뉴를 선택하게 되며, 인증서를 잠시 정지시키고자 하는 경우에는 인증서 정지 메뉴를 선택하게 되며, 상기 정지시킨 인증서를 다시 회복시키고자 하는 경우에는 인증서 회복 메뉴를 선택하게 되는 것이다.

<30> 그러면 사용자 시스템(104)은 (S402)단계에서 생체정보의 입력을 요구하여 사용자 시스템(104)에 연결된 생체정보 입력장치 중 하나인 지문정보 입력장치(102)를 통해 입력되는 사용자 고유의 지문정보를 입력받는다. 이어 사용자 시스템(104)은 (S404)단계로 진행해서 상기 사용자 생체정보가 포함된 인증서 변경 요청 메시지를 생성하여 상기 인증기관(108)의 공개키로 암호화하고, (S506)단계로 진행해서 인터넷(106)을 통해 상기 인증서 변경 요청 메시지를 상기 인증기관(108)으로 전송시키게 된다.

<31> 도 5는 본 발명의 실시 예에 따른 공개키 기반 구조 인증시스템의 인증기관에서 생체정보를 이용하여 회원 사용자에 대한 인증서 권한 변경을 수행하는 동작 제어 흐름을 도시한 것이다. 이하 상기 도 1, 도 3 및 도 5를 참조하여 본 발명의 실시 예를 상세히 설명한다.

<32> 먼저 인터넷(106)을 통해 연결된 상기 사용자 시스템(104)으로부터 인증서 권한 변경 요청 메시지를 수신하는 경우 인증기관(108)의 서버 제어부(302)는 (S500)단계에서 이에 응답하여 (S502)단계로 진행해서 상기 분석 모듈부(300)를 제어하여 상기 사용자 시스템(104)으로부터 암호화되어 전송된 인증서 권한 변경 요청 메시지를 복호화시키고 상기 회원 사용자의 전자서명을 분석하여 인증서 권한 변경 요청 정보의 무결성을 검사하며, 이어 (S504)단계로 진행해서 상기 인증서 권한 변경 요청 메시지 포함된 사용자의 생체정보가 데이터 베이스 저장부(110)내 생체정보 DB(312)에 저장된 해당 사용자의 생체정보와 일치하는지 여부를 검사한다.

<33> 이때 만일 상기 인증서 권한 변경 요청 메시지의 무결성에 문제가 발생하거나 상기 수신된 사용자의 지문정보가 생체정보 DB(312)내 저장된 해당 사용자의 미리 등록된 지문정보와 일치하지 않는 경우 인증기관 서버 제어부(302)는 상기 (S506)단계에서 이에 응답하여 (S507)단계로 진행해서 상기 메시지 생성모듈부(304)를 제어하여 상기 인증서 권한 변경 요청을 정상적으로 수행할 수 없음을 알리는 인증서 권한 변경 오류 메시지를 생성하여 사용자 시스템(104)으로 전송시킨다.

<34> 그러나 이와 달리 상기 인증서 권한 변경 요청 메시지의 무결성에 문제가 없고, 상기 입력된 사용자의 지문정보가 생체정보 DB(312)내 저장된 해당 사용자의 미리 등록된 지문정보와 일치하는지 경우 인증기관 서버 제어부(302)는 상기 (S506)단계에서 이에 응답하여 (S508)단계로 진행해서 상기 인증서 권한 변경 요

청 메시지가 인증서의 폐지를 요구하는 것인지, 인증서의 정지를 요구하는 것인지, 인증서의 회복을 요구하는 것인지 여부를 검사한다.

<35> 즉, 이때 만일 상기 인증서 변경 요청 메시지가 인증서의 폐지를 요구하는 메시지인 경우 인증기관 서버 제어부(302)는 (S510)단계에서 이에 응답하여 (S512)단계로 진행해서 상기 회원 사용자의 인증서를 정상적으로 폐지 처리하고, (S514)단계에서 메시지 생성모듈부(304)를 제어하여 인증서 폐지 요청이 정상 처리되었음을 알리는 응답메시지를 생성시킨다. 이와 달리 상기 인증서 변경 요청 메시지가 인증서의 중지를 요구하는 메시지인 경우 인증기관 서버 제어부(302)는 (S516)단계에서 이에 응답하여 (S518)단계로 진행해서 상기 회원 사용자의 인증서를 정상적으로 정지 처리하고, 상기 (S514)단계에서 메시지 생성모듈부(304)를 제어하여 인증서 중지 요청이 정상 처리되었음을 알리는 응답메시지를 생성시킨다. 그리고 이와 달리 상기 인증서 변경 요청 메시지가 중지되었던 인증서의 회복을 요구하는 메시지인 경우 인증기관 서버 제어부(302)는 (S520)단계에서 이에 응답하여 (S522)단계로 진행해서 상기 회원 사용자의 인증서 권한이 정상적으로 회복되도록 처리하고, 상기 (S514)단계에서 메시지 생성모듈부(304)를 제어하여 인증서 회복 요청이 정상 처리되었음을 알리는 응답메시지를 생성시킨다.

<36> 이어 인증기관 서버 제어부(302)는 (S524)단계로 진행해서 상기 인증서 권한 변경 요청 메시지의 처리에 따라 생성된 해당 응답메시지를 상기 사용자 시스템(104)의 공개키로 암호화하고 인증기관(108)의 개인키로 전자서명하여 해당 사용자 시스템(104)으로 전송시키게 된다.

<37> 따라서 상기한 바와 같이 공개키 기반 구조 인증시스템에서 생체정보를 이용한 보다 신뢰성 높은 사용자 인증을 통해 사용자 시스템과 인증기관간 온라인으로 인증서 권한 변경이 수행될 수 있게 된다.

<38> 한편 상술한 본 발명의 설명에서는 구체적인 실시 예에 관해 설명하였으나, 여러 가지 변형이 본 발명의 범위에서 벗어나지 않고 실시할 수 있다. 따라서 발명의 범위는 설명된 실시 예에 의하여 정할 것이 아니고 특허청구범위에 의해 정하여져야 한다.

【발명의 효과】

<39> 이상에서 설명한 바와 같이, 본 발명은 공개키 기반 구조 인증시스템에서 인증서의 폐지, 중지, 회복 등과 같은 인증서의 권한 변경을 위한 사용자 인증 필요시 생체정보를 이용하여 신뢰성이 보장된 사용자 인증을 수행할 수 있게 됨으로써, 종래와 같이 인증서 권한 변경을 위해 사용자가 등록기관이나 인증기관을 직접 찾아가지 않아도 되며, 인증기관과 온라인 연결된 각자의 사용자 시스템을 이용하여 쉽게 인증서 권한 변경 작업을 수행할 수 있게 되는 이점이 있다.

【특허청구범위】

【청구항 1】

사용자의 신원을 대행 확인하는 등록기관, 상기 등록기관에 의해 신원 확인된 사용자에 대한 인증서를 발행하는 인증기관 및 사용자 시스템을 포함하는 공개키 기반 구조 인증시스템에서 생체정보를 이용하여 발급된 인증서 권한 변경을 요청하는 방법에 있어서,

(a) 상기 인증시스템에 회원 등록된 사용자로부터 인증서 권한 변경 요청이 있는 경우 사용자의 로그인 정보를 이용하여 상기 인증기관 서버에 접속하는 단계;

(b)상기 사용자 시스템에 구비된 생체정보 입력장치를 통해 사용자 인증을 위한 생체정보를 입력받는 단계;

(c) 상기 사용자의 요청에 따른 인증서 권한 변경 요청 메시지를 생성하는 단계; 및

(d)상기 생체정보와 인증서 권한 변경 요청 메시지를 상기 인증기관으로 전송하여 온라인으로 인증서 권한 변경을 요청하는 단계;를 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 2】

제1항에 있어서,

상기 생체정보와 인증서 권한 변경 요청 메시지는, 상기 인증기관의 공개키로 암호화되어 전송되는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 3】

사용자의 신원을 대행 확인하는 등록기관, 상기 등록기관에 의해 신원 확인된 사용자에 대한 인증서를 발행하는 인증기관 및 사용자 시스템을 포함하는 공개키 기반 구조 인증시스템에서 생체정보를 이용하여 발급된 인증서의 권한을 변경 방법에 있어서,

(a') 인터넷을 통해 상기 인증시스템에 접속한 사용자 시스템으로부터의 인증서 권한 변경 요청 메시지를 수신하는 단계;

(b')상기 인증서 권한 변경을 요청한 사용자로부터 시스템 회원 인증을 위한 로그인 정보 및 생체정보를 입력받는 단계;

(c') 상기 개인키를 통해 인증된 사용자의 데이터 베이스 저장부내 등록 생체정보와 상기 입력된 생체정보가 일치하는지 여부를 검사하는 단계;

(d')상기 생체정보가 일치하는 경우 해당 사용자에게 발급된 인증서의 권한을 상기 인증서 권한 변경 요청에 맞게 변경 처리하는 단계; 및

(e')상기 인증서 권한 변경이 정상적으로 처리되었음을 알리는 응답메시지를 상기 사용자 시스템으로 전송하는 단계;를 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 4】

제3항에 있어서,

상기 (a)단계 이후, (a1)상기 인증서 권한 변경 요청 메시지의 무결성을 검사하여 상기 요청 메시지의 무결성에 에러가 발생한 경우에는 인증서 권한 변경 요청을 수행할 수 없음을 알리는 오류발생 메시지를 상기 사용자 시스템으로 전송하는 단계;를 더 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 5】

제3항에 있어서,

상기 (c)단계에서, (c1)상기 데이터 베이스 저장부내 등록 저장된 사용자의 생체정보와 상기 입력된 생체정보가 일치하지 않는 경우에는 회원 사용자 인증 실패를 알리는 오류발생 메시지를 상기 시스템으로 전송하는 단계;를 더 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 6】

제3항에 있어서,

상기 (d)단계에서, (d1)상기 인증서 폐지가 요청된 경우에는 상기 사용자에게 발급된 인증서를 폐지시키는 단계;

(d2)상기 인증서 중지가 요청된 경우에는 상기 사용자에게 발급된 인증서를 중지시키는 단계;

(d3)상기 인증서 회복이 요청된 경우에는 중지 처리된 상기 사용자의 인증서 권한을 회복시키는 단계;를 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 7】

제3항에 있어서,

상기 데이터 베이스 저장부는, 상기 인증시스템에 회원 등록된 사용자 정보를 구비한 사용자 정보 DB와 상기 사용자에 대한 생체정보를 저장하고 있는 생체정보 DB를 포함하며, 상기 인증시스템에 등록된 사용자 정보와 해당 사용자의 생체정보를 연계하여 등록 저장하고 있는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 8】

제1항 또는 제3항에 있어서,

상기 사용자 시스템은, 사용자의 생체정보 입력을 위한 생체정보 입력장치를 구비하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 9】

제1항 또는 제3항에 있어서,

상기 생체정보는, 상기 사용자 고유의 지문 정보인 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【청구항 10】

제1항 또는 제3항에 있어서,

상기 생체정보는, 상기 사용자 고유의 홍체 정보인 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

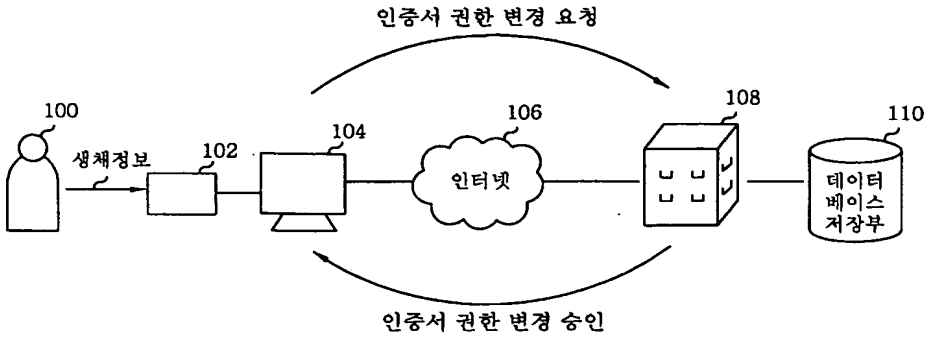
【청구항 11】

제1항 또는 제3에 있어서,

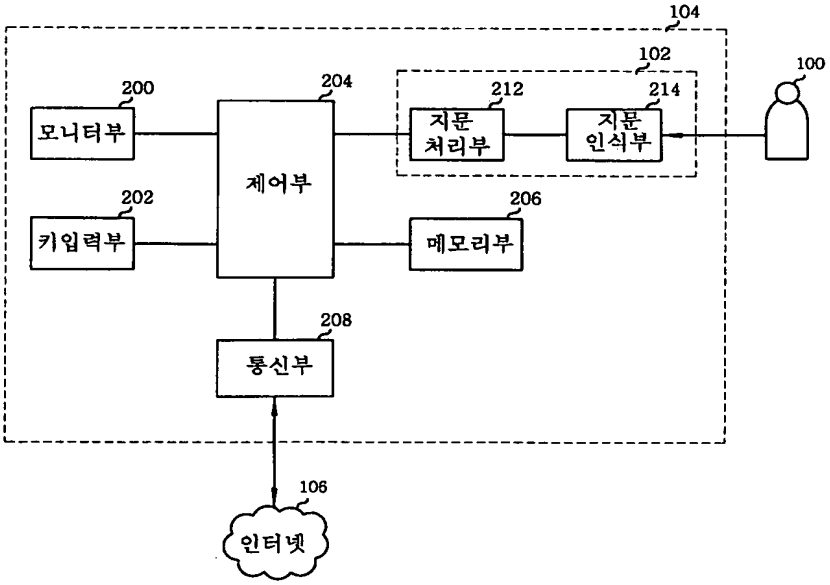
상기 생체정보는, 상기 사용자 고유의 얼굴 특징 벡터 정보인 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 권한 변경 방법.

【도면】

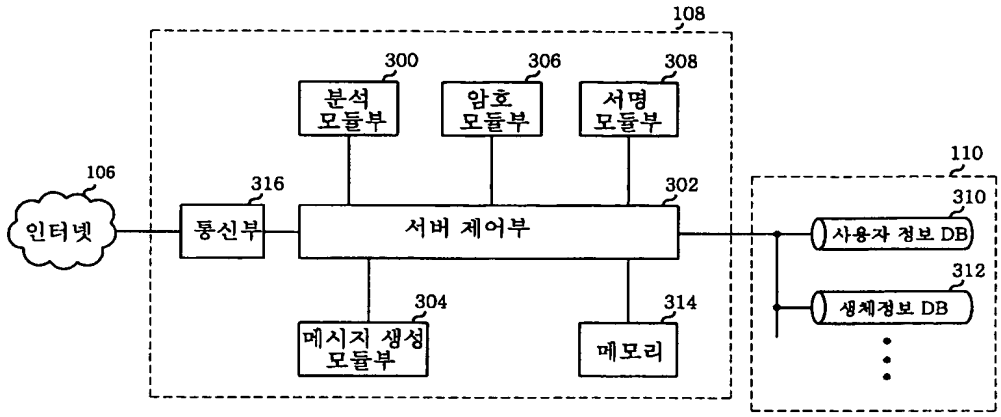
【도 1】


인증서 권한 변경 요청
100
생체정보
102
104
106
인터넷
108
110
데이터 베이스 저장부
인증서 권한 변경 승인

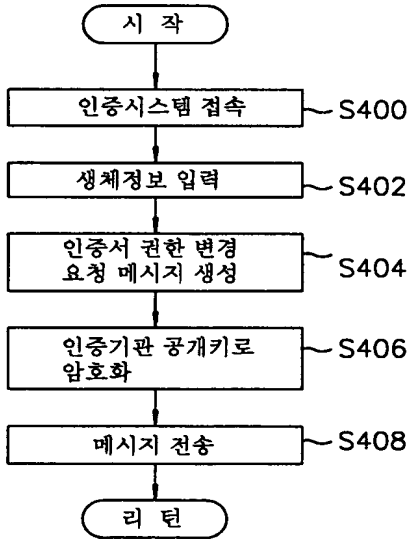
【도 2】


104
102
100
200
204
212
214
모니터부
제어부
지문 처리부
지문 인식부
202
206
키입력부
메모리부
208
통신부
106
인터넷

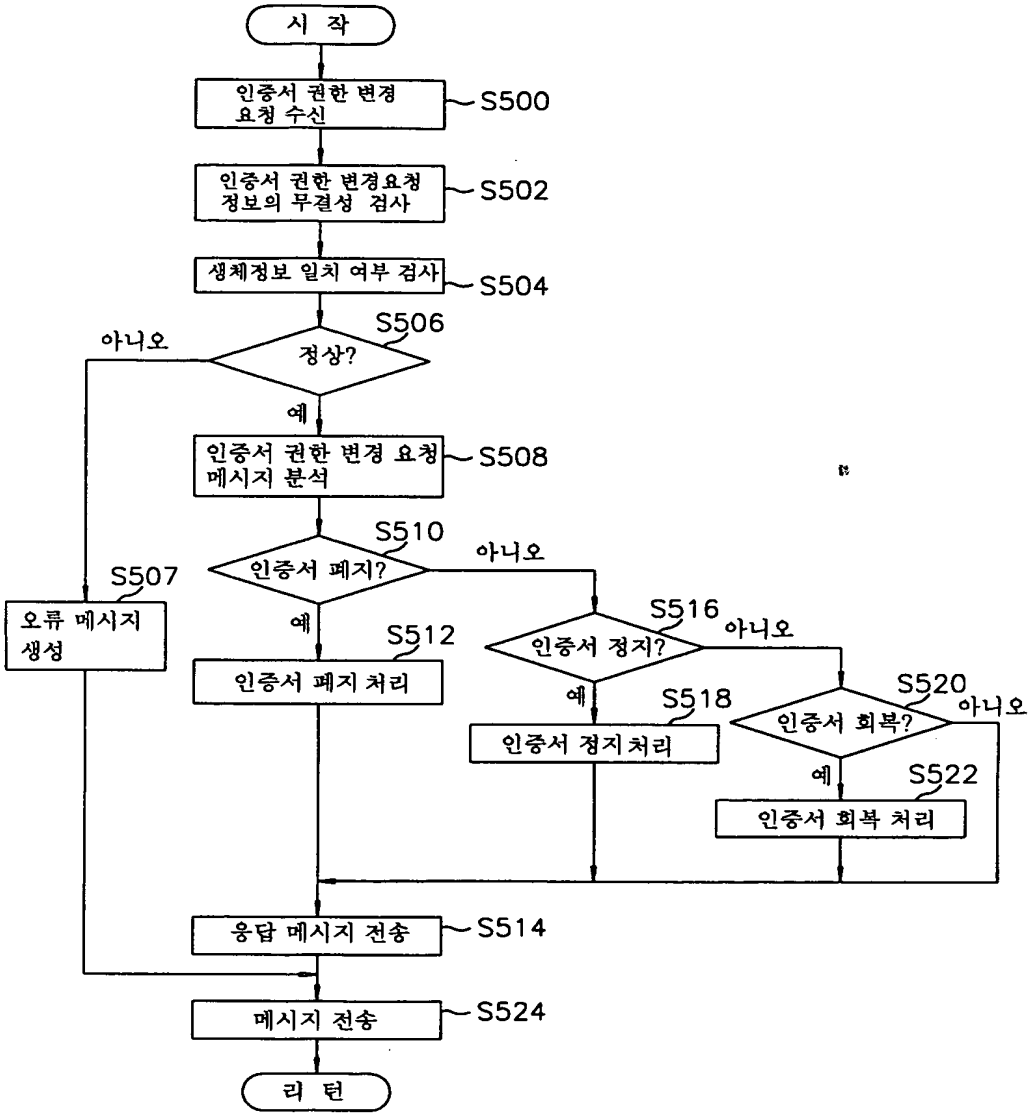
【도 3】


108
300
분석 모듈부
306
암호 모듈부
308
서명 모듈부
106
인터넷
316
통신부
서버 제어부
302
110
310
사용자 정보 DB
312
생체정보 DB
304
메시지 생성 모듈부
314
메모리

【도 4】


시 작
인증시스템 접속
S400
생체정보 입력
S402
인증서 권한 변경 요청 메시지 생성
S404
인증기관 공개키로 암호화
S406
메시지 전송
S408
리 턴

【도 5】


시 작
인증서 권한 변경 요청 수신
S500
인증서 권한 변경요청 정보의 무결성 검사
S502
생체정보 일치 여부 검사
S504
S506
정상?
아니오
예
인증서 권한 변경 요청 메시지 분석
S508
S510
인증서 폐지?
아니오
S507
오류 메시지 생성
예
S512
인증서 폐지 처리
S516
인증서 정지?
아니오
예
S518
인증서 정지처리
S520
인증서 회복?
아니오
예
S522
인증서 회복 처리
응답 메시지 전송
S514
메시지 전송
S524
리 턴